(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) **EP 3 400 541 B1**

(12) **EUROPEAN PATENT SPECIFICATION**

(45) Date of publication and mention of the grant of the patent:
21.10.2020 Bulletin 2020/43

(21) Application number: **16897290.9**

(22) Date of filing: **29.03.2016**

(51) Int Cl.:
G06Q 20/36 *(2012.01)* ***G06Q 20/38*** *(2012.01)*
H04L 29/06 *(2006.01)*

(86) International application number:
PCT/US2016/024776

(87) International publication number:
WO 2017/171733 (05.10.2017 Gazette 2017/40)

(54) SYSTEMS AND METHODS FOR PROVIDING BLOCK CHAIN-BASED MULTIFACTOR PERSONAL IDENTITY VERIFICATION

SYSTEME UND VERFAHREN ZUR BEREITSTELLUNG BLOCKKETTENBASIERTER MULTIFAKTORIELLER PERSÖNLICHER IDENTITÄTSPRÜFUNG

SYSTÈMES ET PROCÉDÉS DE FOURNITURE D'UNE VÉRIFICATION D'IDENTITÉ PERSONNELLE MULTIFACTORIELLE BASÉE SUR UNE CHAÎNE DE BLOCS

(84) Designated Contracting States:
AL AT BE BG CH CY CZ DE DK EE ES FI FR GB GR HR HU IE IS IT LI LT LU LV MC MK MT NL NO PL PT RO RS SE SI SK SM TR

(30) Priority: **28.03.2016 US 201615083241**

(43) Date of publication of application:
14.11.2018 Bulletin 2018/46

(60) Divisional application:
18206468.3 / 3 483 814
18206477.4 / 3 483 815
18206482.4 / 3 486 854
18206522.7 / 3 483 816
18206524.3 / 3 483 817

(73) Proprietor: **Black Gold Coin, Inc.**
Las Vegas, Nevada 89130 (US)

(72) Inventor: **ANDRADE, Marcus**
Las Vegas, NV 89130 (US)

(74) Representative: **Kretschmann, Dennis**
Boehmert & Boehmert
Anwaltspartnerschaft mbB
Pettenkoferstrasse 22
80336 München (DE)

(56) References cited:
WO-A2-2015/183901
US-A1- 2012 084 563
US-A1- 2015 178 693
US-A1- 2015 324 789
US-A1- 2015 324 789
US-A1- 2015 356 555

EP 3 400 541 B1

Description

FIELD OF THE DISCLOSURE

[0001] This disclosure relates to systems and methods for providing block chain-based multifactor personal identity verification.

[0002] US application US 2015/0324789 A1 discloses virtual wallets used to store and execute transactions using cryptocurrency. The security of the cryptocurrency transaction is enhanced by utilizing three encryption keys stored in three different locations to secure the wallet.

[0003] International publication WO 2015/183901 A2 relates to a marketplace software platform that provides the capability for negotiation of retail item prices or the issuance of electronic discounts.

SUMMARY

[0004] According to the present invention there is provided a system according to claim 1, and a method as in claim 8. Embodiments are further defined by the dependent claims.

[0005] These and other features, and characteristics of the present technology, as well as the methods of operation and functions of the related elements of structure and the combination of parts and economies of manufacture, will become more apparent upon consideration of the following description and the appended claims with reference to the accompanying drawings, all of which form a part of this specification, wherein like reference numerals designate corresponding parts in the various figures. It is to be expressly understood, however, that the drawings are for the purpose of illustration and description only and are not intended as a definition of the limits of the invention. As used in the specification and in the claims, the singular form of "a", "an", and "the" include plural referents unless the context clearly dictates otherwise.

BRIEF DESCRIPTION OF THE DRAWINGS

[0006]

FIG. 1 illustrates a system for providing block chain-based multifactor personal identity verification, in accordance with one or more implementations.

FIG. 2 illustrates a method for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, in accordance with one or more implementations.

FIG. 3 illustrates a method for performing block chain-based multifactor personal identity verification using verification addresses, in accordance with one or more implementations.

DETAILED DESCRIPTION

[0007] FIG. 1 illustrates a system 100 for providing block chain-based multifactor personal identity verification, in accordance with one or more implementations. In some implementations, system 100 may include one or more servers 102. The server(s) 102 may be configured to communicate with one or more computing platforms 104 according to a client/server architecture, a peer-to-peer architecture, and/or other architectures. The users may access system 100 via computing platform(s) 104.

[0008] The server(s) 102 may be configured to execute machine-readable instructions 106. The machine-readable instructions 106 may include one or more of an individual identifier component 108, a verification address assignment component 110, an address recordation component 112, a user interface component 114, a verification request component 116, an information extraction component 118, an identity verification component 120, and/or other machine-readable instruction components.

[0009] The machine-readable instructions 106 may be executable to establish verification addresses on a block chain. Generally speaking, a block chain is a transaction database shared by some or all nodes participating in system 100. Such participation may be based on the Bitcoin protocol, Ethereum protocol, and/or other protocols related to digital currencies and/or block chains. A full copy of the block chain contains every transaction ever executed in an associated digital currency. In addition to transactions, other information may be contained by the block chain, such as described further herein.

[0010] The block chain may be based on several blocks. A block may include a record that contains and confirms one or more waiting transactions. Periodically (e.g., roughly every one minute), a new block including transactions and/or other information may be appended to the block chain. In some implementations, a given block in the block chain contains a hash of the previous block. This may have the effect of creating a chain of blocks from a genesis block (i.e., the first block in the block chain) to a current block. The given block may be guaranteed to come chronologically after a previous block because the previous block's hash would otherwise not be known. The given block may be computationally impractical to modify once it is included in the block chain because every block after it would also have to be regenerated.

[0011] A given verification address may include a specific location on the block chain where certain information is stored. In some implementations, an individual verification address may be referred to as an "AtenVerify Address." Verification addresses are further described below in connection with verification address assignment component 110.

[0012] The individual identifier component 108 may be configured to associated identifiers with individuals hav-

ing previously verified personal identities. For example, a first identifier may be associated a first individual. The first individual may have a previously verified personal identity. Generally speaking, an identifier may include one or more of a number, an alphanumeric code, a username, and/or other information that can be linked to an individual. In some implementations, an individual identifier may be referred to as an "Aten ID."

[0013] In accordance with some implementations, an individual having a previously verified personal identity may have obtained the previously verified personal identity through a variety of approaches. For example, in some implementations the individual may be required to provide evidence of the individual's identity. Such evidence may include one or more of providing a copy of a government issued identification (e.g., passport and/or driver's license), providing a copy of mail received by the individual (e.g., a utility bill), evidence provided by a third party, and/or other evidence on an individual's identity. The evidence may be provided to an entity associated with server(s) 102.

[0014] The verification address assignment component 110 may be configured to assign verification addresses on a block chain to the individuals. A given verification address may include a public key and a private key. By way of example, a first verification address may be assigned to the first individual. The first verification address may include a first public key and a first private key.

[0015] Generally speaking, a public and private keypair may be used for encryption and decryption according to one or more public key algorithms. By way of nonlimiting example, a key pair may be used for digital signatures. Such a key pair may include a private key for signing and a public key for verification. The public key may be widely distributed, while the private key is kept secret (e.g., known only to its proprietor). The keys may be related mathematically, but calculating the private key from the public key is unfeasible.

[0016] In some implementations, verification address assignment component 110 may be configured such that private keys may be stored within computing platform(s) 104. For example, the first private key may be stored within a computing platform 104 and/or other locations associated with the first individual. In accordance with some implementation, a private key may be stored in one or more of a "verify.dat" file, a SIM card, and/or other locations.

[0017] In some implementations, verification address assignment component 110 may be configured such that multiple verification addresses may be assigned to separate individuals. For example, in addition to the first verification address, a second verification address may be assigned to the first individual. One or more additional verification addresses may be assigned to the first individual, in accordance with one or more implementations.

[0018] The address recordation component 112 may be configured to record identifiers and biometric data associated with the individuals at corresponding verification addresses. For example, the first identifier and first biometric data associated with the first individual may be recorded at the first verification address. Recording information at a given verification address may include recording a hash or other encrypted representation of the information. In some implementations, different biometric data may be recorded at multiple verification addresses assigned to a single given individual. For example, in addition to the first identifier and the first biometric data associated with the first individual being recorded at the first verification address, the first identifier and second biometric data associated with the first individual may be recorded at a second verification address.

[0019] Generally speaking, biometric data may include metrics related to human characteristics. Biometric identifiers are distinctive, measurable characteristics that can be used to label and describe individuals. Biometric identifiers are typically include physiological characteristics, but may also include behavioral characteristics and/or other characteristics. Physiological characteristics may be related to the shape of an individual's body. Examples of physiological characteristics used as biometric data may include one or more of fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor or scent, and/or other physiological characteristics. Behavioral characteristics may be related to a pattern of behavior of an individual. Examples of behavioral characteristics used as biometric data may include one or more of typing rhythm, gait, voice, and/or other behavioral characteristics.

[0020] The biometric data may include one or more of an image or other visual representation of a physiological characteristic, a recording of a behavioral characteristic, a template of a physiological characteristic and/or behavioral characteristic, and/or other biometric data. A template may include a synthesis of relevant features extracted from the source. A template may include one or more of a vector describing features of a physiological characteristic and/or behavioral characteristic, a numerical representation of a physiological characteristic and/or behavioral characteristic, an image with particular properties, and/or other information.

[0021] Biometric data may be received via computing platforms 104 associated with the individuals. For example, biometric data associated with a first individual may be received via a first computing platform 104 associated with the first individual. The first computing platform 104 may include an input device (not depicted) configured to capture and/or record a physiological characteristic and/or behavioral characteristic of the first individual. Examples of such an input device may include one or more of a camera and/or other imaging device, a fingerprint scanner, a microphone, an accelerometer, and/or other input devices.

[0022] The user interface component 114 may be configured to provide an interface for presentation to individuals via associated computing platforms 104. The inter-

face may include a graphical user interface presented via individual computing platforms 104. According to some implementations, the interface may be configured to allow a given individual to add or delete verification addresses assigned to the given individual so long as at least one verification address is assigned to the given individual.

[0023] In some implementations, user interface component 114 may be configured to access and/or manage one or more user profiles and/or user information associated with users of system 100. The one or more user profiles and/or user information may include information stored by server(s) 102, one or more of the computing platform(s) 104, and/or other storage locations. The user profiles may include, for example, information identifying users (e.g., a username or handle, a number, an identifier, and/or other identifying information), security login information (e.g., a login code or password), system account information, subscription information, digital currency account information (e.g., related to currency held in credit for a user), relationship information (e.g., information related to relationships between users in system 100), system usage information, demographic information associated with users, interaction history among users in the system 100, information stated by users, purchase information of users, browsing history of users, a computing platform identification associated with a user, a phone number associated with a user, and/or other information related to users.

[0024] The machine-readable instructions 106 may be executable to perform block chain-based multifactor personal identity verification using the verification addresses.

[0025] The verification request component 116 may be configured to receive one or more identifiers in connection with one or more requests to verify an identity of one or more individuals. For example, the first identifier may be received in connection with a request to verify an identity of the first individual. Requests for identity verification may be provided in connection with and/or related to financial transactions, information exchanges, and/or other interactions. Requests may be received from other individuals and/or other third parties.

[0026] The information extraction component 118 may be configured to extract the biometric data associated with the one or more individuals from the corresponding verification addresses. For example, the first biometric data associated with the first individual may be extracted from the first verification address. Extracting information (e.g., biometric data) from a verification address may include decrypting information.

[0027] According to some implementations, information extraction component 118 may be configured such that, responsive to receiving the request to verify the identity of the first individual, a prompt may be provided to the first individual for biometric data matching the first biometric data and a private key matching the first private key. The prompt may be conveyed via a computing platform 104 associated with the first individual. The prompt may be conveyed via a graphical user interface and/or other user interface provided by the computing platform 104 associated with the first individual. The prompt may include an indication that is one or more of visual, audible, haptic, and/or other indications.

[0028] In some implementations, information extraction component 118 may be configured such that, responsive to receiving the request to verify the identity of the first individual, a prompt may be provided to a computing platform 104 associated with the first individual. The prompt may cause the computing platform 104 to automatically provide, to server(s) 102, biometric data matching the first biometric data and/or a private key matching the first private key.

[0029] The identity verification component 120 may be configured to verify the identity of the one or more individuals upon, or in response to, receiving matching biometric data and private keys. For example, the personal identity of the first individual may be verified upon receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Verifying the personal identity of the first individual may include comparing stored information with newly received information.

[0030] According to some implementations, identity verification component 120 may be configured such that the personal identity of the first individual may be verified upon receipt of (1) biometric data matching the first biometric data or the second biometric data and (2) a private key matching the first private key. Such implementations may provide so-called "M-of-N" signatures for identity verification where some subset of a larger set of identifying information is required.

[0031] In some implementations, identity verification component 120 may be configured such that the biometric data matching the first biometric data and the private key matching the first private key may be used to sign the verification of the personal identity of the first individual.

[0032] A cryptographic signature is a mathematical mechanism that allows someone to prove ownership. In the case of Bitcoin, a Bitcoin wallet and its private key(s) are linked by some mathematical magic. When your Bitcoin software signs a transaction with the appropriate private key, the whole network can see that the signature matches the bitcoins being spent. However, there is no way for the world to guess your private key to steal your hard-earned bitcoins.

[0033] In some implementations, at least one dedicated node performs the signing of the verification of the personal identity of the first individual. A given dedicated node may include one or more of the server(s) 102. The given dedicated node may be a public node or a private node configured for creating new blocks and/or for signing verification.

[0034] In some implementations, server(s) 102, computing platform(s) 104, and/or external resources 122

may be operatively linked via one or more electronic communication links. For example, such electronic communication links may be established, at least in part, via a network such as the Internet and/or other networks. It will be appreciated that this is not intended to be limiting, and that the scope of this disclosure includes implementations in which server(s) 102, computing platform(s) 104, and/or external resources 122 may be operatively linked via some other communication media.

[0035] A given computing platform 104 may include one or more processors configured to execute machine-readable instructions. The machine-readable instructions may be configured to enable an expert or user associated with the given computing platform 104 to interface with system 100 and/or external resources 122, and/or provide other functionality attributed herein to computing platform(s) 104. By way of non-limiting example, the given computing platform 104 may include one or more of a desktop computer, a laptop computer, a handheld computer, a tablet computing platform, a NetBook, a Smartphone, a gaming console, and/or other computing platforms.

[0036] External resources 122 may include sources of information, hosts and/or providers of virtual environments outside of system 100, external entities participating with system 100, and/or other resources. In some implementations, some or all of the functionality attributed herein to external resources 100 may be provided by resources included in system 100.

[0037] Server(s) 102 may include electronic storage 124, one or more processors 126, and/or other components. Server(s) 102 may include communication lines, or ports to enable the exchange of information with a network and/or other computing platforms. Illustration of server(s) 102 in FIG. 1 is not intended to be limiting. Server(s) 102 may include a plurality of hardware, software, and/or firmware components operating together to provide the functionality attributed herein to server(s) 102. For example, server(s) 102 may be implemented by a cloud of computing platforms operating together as server(s) 102.

[0038] Electronic storage 124 may comprise non-transitory storage media that electronically stores information. The electronic storage media of electronic storage 124 may include one or both of system storage that is provided integrally (i.e., substantially non-removable) with server(s) 102 and/or removable storage that is removably connectable to server(s) 102 via, for example, a port (e.g., a USB port, a firewire port, etc.) or a drive (e.g., a disk drive, etc.). Electronic storage 124 may include one or more of optically readable storage media (e.g., optical disks, etc.), magnetically readable storage media (e.g., magnetic tape, magnetic hard drive, floppy drive, etc.), electrical charge-based storage media (e.g., EEPROM, RAM, etc.), solid-state storage media (e.g., flash drive, etc.), and/or other electronically readable storage media. Electronic storage 124 may include one or more virtual storage resources (e.g., cloud storage, a virtual private network, and/or other virtual storage resources). Electronic storage 124 may store software algorithms, information determined by processor(s) 126, information received from server(s) 102, information received from computing platform(s) 104, and/or other information that enables server(s) 102 to function as described herein.

[0039] Processor(s) 126 may be configured to provide information processing capabilities in server(s) 102. As such, processor(s) 126 may include one or more of a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information. Although processor(s) 126 is shown in FIG. 1 as a single entity, this is for illustrative purposes only. In some implementations, processor(s) 126 may include a plurality of processing units. These processing units may be physically located within the same device, or processor(s) 126 may represent processing functionality of a plurality of devices operating in coordination. The processor(s) 126 may be configured to execute machine-readable instruction components 108, 110, 112, 114, 116, 118, 120, and/or other machine-readable instruction components. Processor(s) 126 may be configured to execute machine-readable instruction components 108, 110, 112, 114, 116, 118, 120, and/or other machine-readable instruction components by software; hardware; firmware; some combination of software, hardware, and/or firmware; and/or other mechanisms for configuring processing capabilities on processor(s) 126. As used herein, the term "machine-readable instruction component" may refer to any component or set of components that perform the functionality attributed to the machine-readable instruction component. This may include one or more physical processors during execution of processor readable instructions, the processor readable instructions, circuitry, hardware, storage media, or any other components.

[0040] It should be appreciated that although machine-readable instruction components 108, 110, 112, 114, 116, 118, and 120 are illustrated in FIG. 1 as being implemented within a single processing unit, in implementations in which processor(s) 126 includes multiple processing units, one or more of machine-readable instruction components 108, 110, 112, 114, 116, 118, and/or 120 may be implemented remotely from the other machine-readable instruction components. The description of the functionality provided by the different machine-readable instruction components 108, 110, 112, 114, 116, 118, and/or 120 described below is for illustrative purposes, and is not intended to be limiting, as any of machine-readable instruction components 108, 110, 112, 114, 116, 118, and/or 120 may provide more or less functionality than is described. For example, one or more of machine-readable instruction components 108, 110, 112, 114, 116, 118, and/or 120 may be eliminated, and some or all of its functionality may be provided by other

ones of machine-readable instruction components 108, 110, 112, 114, 116, 118, and/or 120. As another example, processor(s) 126 may be configured to execute one or more additional machine-readable instruction components that may perform some or all of the functionality attributed below to one of machine-readable instruction components 108, 110, 112, 114, 116, 118, and/or 120.

[0041] FIG. 2 illustrates a method 200 for establishing verification addresses on a block chain in order to provide block chain-based multifactor personal identity verification, in accordance with one or more implementations. The operations of method 200 presented below are intended to be illustrative. In some implementations, method 200 may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the operations of method 200 are illustrated in FIG. 2 and described below is not intended to be limiting.

[0042] In some implementations, one or more operations of method 200 may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of method 200 in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method 200.

[0043] At an operation 202, identifiers may be associated with individuals having previously verified personal identities. A first identifier may be associated a first individual. The first individual may have a previously verified personal identity. Operation 202 may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to individual identifier component 108 (as described in connection with FIG. 1), in accordance with one or more implementations.

[0044] At an operation 204, verification addresses on a block chain may be assigned to the individuals. A given verification address may include a public key and a private key. A first verification address may be assigned to the first individual. The first verification address may include a first public key and a first private key. Operation 204 may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to verification address assignment component 110 (as described in connection with FIG. 1), in accordance with one or more implementations.

[0045] At an operation 206, identifiers and biometric data associated with the individuals may be recorded at corresponding verification addresses. The first identifier and first biometric data associated with the first individual may be recorded at the first verification address. The identity of the one or more individuals may be verifiable upon, or in response to, receiving matching biometric data and private keys. The personal identity of the first individual may be verifiable upon, or in response to, receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Operation 206 may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to address recordation component 112 (as described in connection with FIG. 1), in accordance with one or more implementations.

[0046] FIG. 3 illustrates a method 300 for performing block chain-based multifactor personal identity verification using verification addresses, in accordance with one or more implementations. The operations of method 300 presented below are intended to be illustrative. In some implementations, method 300 may be accomplished with one or more additional operations not described, and/or without one or more of the operations discussed. Additionally, the order in which the operations of method 300 are illustrated in FIG. 3 and described below is not intended to be limiting.

[0047] In some implementations, method 300 may be implemented in one or more processing devices (e.g., a digital processor, an analog processor, a digital circuit designed to process information, an analog circuit designed to process information, a state machine, and/or other mechanisms for electronically processing information). The one or more processing devices may include one or more devices executing some or all of the operations of method 300 in response to instructions stored electronically on an electronic storage medium. The one or more processing devices may include one or more devices configured through hardware, firmware, and/or software to be specifically designed for execution of one or more of the operations of method 300.

[0048] At an operation 302, one or more identifiers may be received in connection with one or more requests to verify an identity of one or more individuals. A first identifier may be received in connection with a request to verify an identity of a first individual. Operation 302 may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to verification request component 116 (as described in connection with FIG. 1), in accordance with one or more implementations.

[0049] At an operation 304, biometric data associated with the one or more individuals may be extracted from corresponding verification addresses on a block chain. A given verification address may include a public key and a private key. First biometric data associated with the first individual may extracted from a first verification address assigned to the first individual. The first verification address may include a first public key and a first private key. Operation 304 may be performed by one or more

hardware processors configured to execute a machine-readable instruction component that is the same as or similar to information extraction component 118 (as described in connection with FIG. 1), in accordance with one or more implementations.

[0050] At an operation 306, the identity of the one or more individuals may be verified upon, or in response to, receiving matching biometric data and private keys. The personal identity of the first individual may be verified upon, or in response to, receipt of (1) biometric data matching the first biometric data and (2) a private key matching the first private key. Operation 306 may be performed by one or more hardware processors configured to execute a machine-readable instruction component that is the same as or similar to identity verification component 120 (as described in connection with FIG. 1), in accordance with one or more implementations.

[0051] Exemplary implementations may facilitate storing personal data on the block chain. The personal data may be stored on the block chain in an encrypted way. A person may be identified at the block chain level with one or more of a private key, a finger print, a finger print hash, an eye retina, an eye retina hash, and/or other unique information. The data stored may include or relate to one or more of a passport, an identification card, extracted passport information, a driver's license, extracted driver's license information, finger print, eye retina, and/or other information. According to some implementations, if some of the data is changed, a new record may be created for that person in the block chain. That is, all changes are added as new records. The old record will always be stored on the block chain. Generally speaking, all records on the block chain are stored forever and cannot be removed. More than one copy of the block chain will exist to ensure the records are not manipulated.

[0052] Exemplary implementations may facilitate access to personal data. There may be multiple access levels for the personal data in the block chain. Access controls may be grated on public/private key pairs levels. Examples of access levels may include one or more of Super Admin (full access to block chain), Authorities-country level (full read-only access), Authorities-state/local level (limited read-only access), Police and other services including Emergency (access to certain personal data by Finger Print/Eye retina of that person only), Participating Merchants (limited access), and/or other access levels.

[0053] Exemplary implementations may facilitate verification check. There may be multiple levels for how it is possible to check verification. For example, some implementations may ensure a person has a record at "Company" but no personal data is provided. Some implementations may ensure a person has a record at Company and get very basic personal information such as Full Name, DOB, Gender, and/or other basic information. Some implementations may ensure a person has a record at Company and get all personal data.

[0054] Although the present technology has been described in detail for the purpose of illustration based on what is currently considered to be the most practical and preferred implementations, it is to be understood that such detail is solely for that purpose and that the technology is not limited to the disclosed implementations. For example, it is to be understood that the present technology contemplates that, to the extent possible, one or more features of any implementation can be combined with one or more features of any other implementation.

Claims

1. A system (100) for providing block chain-based multifactor personal identity verification, the system comprising:

one or more hardware processors (126) configured by machine-readable instructions to:

establish verification addresses on a block chain by:

associating identifiers with individuals having previously verified personal identities, a first identifier being associated with a first individual, the first individual having a previously verified personal identity;

assigning verification addresses on a block chain to the individuals, a given verification address including a specific location on the block chain where information is stored, wherein the given verification address includes a public key and a private key, a first verification address being assigned to the first individual, the first verification address including a first public key and a first private key; and

recording identifiers and biometric data associated with the individuals at corresponding verification addresses, the first identifier and first biometric data associated with the first individual being recorded at the first verification address; and

performing block chain-based multifactor personal identity verification using the verification addresses by:

receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, the first identifier being received in connection with a request to verify an identity of the first individual;

extracting the biometric data associated with the one or more individuals from the corresponding verification addresses, the first biometric data associated with the first

individual being extracted from the first verification address; and
verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) second biometric data matching the first biometric data, and (2) a second private key matching the first private key.

2. The system (100) of claim 1, wherein multiple verification addresses are assigned to separate individuals such that, in addition to the first verification address, a second verification address is assigned to the first individual.

3. The system (100) of any of the preceding claims, wherein different biometric data is recorded at multiple verification addresses assigned to a given individual such that, in addition to the first identifier and the first biometric data associated with the first individual being recorded at the first verification address, the first identifier and third biometric data associated with the first individual is recorded at a third verification address.

4. The system (100) of claim 3, wherein the personal identity of the first individual is verified upon receipt of (1) the second biometric data matching the first biometric data or the third biometric data and (2) the second private key matching the first private key.

5. The system (100) of any of the preceding claims, wherein the biometric data includes one or more of an image, a recording, or a template; and/or
wherein the biometric data is related to one or more of a fingerprint, palm veins, face recognition, DNA, palm print, hand geometry, iris recognition, retina, odor or scent, typing rhythm, gait, or voice.

6. The system (100) of any of the preceding claims, wherein the one or more hardware processors (126) are further configured by machine-readable instructions to, responsive to receiving the request to verify the identity of the first individual, prompt the first individual for the second biometric data matching the first biometric data and the second private key matching the first private key.

7. The system (100) of any of the preceding claims, wherein at least one dedicated node performs the signing of the verification of the personal identity of the first individual, wherein the dedicated node includes one or more servers (102) of the system (100).

8. A method for performing block chain-based multifactor personal identity verification using verification addresses, the method being performed by one or more hardware processors (126) configured by machine-readable instructions, the method comprising:

receiving one or more identifiers in connection with one or more requests to verify an identity of one or more individuals, a first identifier being received in connection with a request to verify an identity of a first individual;
extracting biometric data associated with the one or more individuals from corresponding verification addresses on a block chain, a given verification address including a specific location on the block chain where information is stored, wherein the given verification address includes a public key and a private key, first biometric data associated with the first individual being extracted from a first verification address assigned to the first individual, the first verification address including a first public key and a first private key; and
verifying the identity of the one or more individuals upon receiving matching biometric data and private keys, the personal identity of the first individual being verified upon receipt of (1) second biometric data matching the first biometric data, and (2) a second private key matching the first private key.

9. The method of claim 8, further comprising, responsive to receiving the request to verify the identity of the first individual:

prompting the first individual for the second biometric data matching the first biometric data and the second private key matching the first private key, the prompt being conveyed via a computing platform (104) associated with the first individual; or
prompting a computing platform (104) associated with the first individual to automatically provide the second biometric data matching the first biometric data and the second private key matching the first private key.

Patentansprüche

1. System (100) zur Bereitstellung einer Blockketten-basierten Multifaktor-Identitätsprüfung von Personen, wobei das System Folgendes umfasst:
einen oder mehrere Hardwareprozessoren (126), die durch maschinenlesbare Anweisungen zu Folgendem konfiguriert sind:

Einrichten von Verifizierungsadressen in einer Blockkette durch:

Assoziieren von Identifikatoren mit Individuen, die zuvor verifizierte persönliche Identitäten aufweisen, wobei ein erster Identifikator mit einem ersten Individuum assoziiert wird, wobei das erste Individuum eine zuvor verifizierte persönliche Identität aufweist;
Zuweisen von Verifizierungsadressen in einer Blockkette zu den Individuen, wobei eine gegebene Verifizierungsadresse einen spezifischen Ort auf der Blockkette umfasst, an welchem Informationen gespeichert werden, wobei die gegebene Verifizierungsadresse einen öffentlichen Schlüssel und einen privaten Schlüssel aufweist, wobei eine erste Verifizierungsadresse dem ersten Individuum zugewiesen ist, wobei die erste Verifizierungsadresse einen ersten öffentlichen Schlüssel und einen ersten privaten Schlüssel aufweist; und
Aufzeichnen von Identifikatoren und biometrischen Daten, die mit den Individuen assoziiert sind, an entsprechenden Verifizierungsadressen, wobei der erste Identifikator und erste biometrische Daten, die mit dem ersten Individuum assoziiert sind, an der ersten Verifizierungsadresse aufgezeichnet werden; und

Durchführen einer Blockketten-basierten Multifaktor-Identitätsprüfung von Personen unter Verwendung der Verifizierungsadressen durch:

Empfangen eines oder mehrerer Identifikatoren in Verbindung mit einer oder mehreren Anfragen zur Verifizierung einer Identität eines oder mehrerer Individuen, wobei der erste Identifikator in Verbindung mit einer Anfrage zur Verifizierung einer Identität des ersten Individuums empfangen wird;
Extrahieren der biometrischen Daten, die mit dem einen oder den mehreren Individuen assoziiert sind, aus den entsprechenden Verifizierungsadressen, wobei die ersten biometrischen Daten, die mit dem ersten Individuum assoziiert sind, aus der ersten Verifizierungsadresse extrahiert werden; und
Verifizieren der Identität des einen oder der mehreren Individuen bei Empfang passender biometrischer Daten und privater Schlüssel, wobei die persönliche Identität des ersten Individuums bei Empfang (1) zweiter biometrischer Daten, die zu den ersten biometrischen Daten passen, und (2) eines zweiten privaten Schlüssels, der zu dem ersten privaten Schlüssel passt, verifiziert wird.

2. System (100) gemäß Anspruch 1, wobei mehrere Verifizierungsadressen separaten Individuen zugewiesen sind, derart, dass zusätzlich zu der ersten Verifizierungsadresse dem ersten Individuum eine zweite Verifizierungsadresse zugewiesen ist.

3. System (100) gemäß einem der vorhergehenden Ansprüche, wobei unterschiedliche biometrische Daten an mehreren Verifizierungsadressen, die einem gegebenen Individuum zugewiesen sind, aufgezeichnet sind, derart, dass zusätzlich zu dem ersten Identifikator und den ersten biometrischen Daten, die mit dem ersten Individuum assoziiert sind und die an der ersten Verifizierungsadresse aufgezeichnet sind, der erste Identifikator und dritte biometrische Daten, die mit dem ersten Individuum assoziiert sind, an einer dritten Verifizierungsadresse aufgezeichnet sind.

4. System (100) gemäß Anspruch 3, wobei die persönliche Identität des ersten Individuums bei Empfang (1) der zweiten biometrischen Daten, die zu den ersten biometrischen Daten oder zu den dritten biometrischen Daten passen, und (2) des zweiten privaten Schlüssels, der zu dem ersten privaten Schlüssel passt, verifiziert wird.

5. System (100) gemäß einem der vorhergehenden Ansprüche, wobei die biometrischen Daten eines oder mehrere aus einem Bild, einer Aufzeichnung oder einer Vorlage beinhalten; und/oder
wobei sich die biometrischen Daten auf eines oder mehrere aus einem Fingerabdruck, Handflächenvenen, Gesichtserkennung, DNA, Handflächenabdruck, Handgeometrie, Iriserkennung, Retina, Geruch oder Duft, Tipprhythmus, Gang oder Stimme beziehen.

6. System (100) gemäß einem der vorhergehenden Ansprüche, wobei der eine oder die mehreren Hardwareprozessoren (126) ferner durch maschinenlesbare Anweisungen zum Auffordern des ersten Individuums zur Bereitstellung der zweiten biometrischen Daten, die zu den ersten biometrischen Daten passen, und des zweiten privaten Schlüssels, der zu dem ersten privaten Schlüssel passt, als Reaktion auf das Empfangen der Anfrage zur Verifizierung der Identität des ersten Individuums eingerichtet sind.

7. System (100) gemäß einem der vorhergehenden Ansprüche, wobei mindestens ein dedizierter Knoten die Signierung der Verifizierung der persönlichen Identität des ersten Individuums durchführt, wobei der dedizierte Knoten einen oder mehrere Server (102) des Systems (100) umfasst.

8. Verfahren zum Durchführen einer Blockketten-basierten Multifaktor-Identitätsprüfung von Personen unter Verwendung von Verifizierungsadressen, wo-

bei das Verfahren durch einen oder mehrere Hardwareprozessoren (126) durchgeführt wird, die durch maschinenlesbare Anweisungen konfiguriert werden, wobei das Verfahren Folgendes umfasst:

Empfangen eines oder mehrerer Identifikatoren in Verbindung mit einer oder mehreren Anfragen zur Verifizierung einer Identität eines oder mehrerer Individuen, wobei ein erster Identifikator in Verbindung mit einer Anfrage zur Verifizierung einer Identität eines ersten Individuums empfangen wird;
Extrahieren biometrischer Daten, die mit dem einen oder den mehreren Individuen assoziiert sind, aus entsprechenden Verifizierungsadressen in einer Blockkette, wobei eine gegebene Verifizierungsadresse einen spezifischen Ort auf der Blockkette umfasst, an welchem Informationen gespeichert werden, wobei die gegebene Verifizierungsadresse einen öffentlichen Schlüssel und einen privaten Schlüssel aufweist, wobei erste biometrische Daten, die mit dem ersten Individuum assoziiert sind, aus einer ersten Verifizierungsadresse extrahiert werden, die dem ersten Individuum zugewiesen ist, wobei die erste Verifizierungsadresse einen ersten öffentlichen Schlüssel und einen ersten privaten Schlüssel aufweist; und
Verifizieren der Identität des einen oder der mehreren Individuen bei Empfang passender biometrischer Daten und privater Schlüssel, wobei die persönliche Identität des ersten Individuums bei Empfang (1) zweiter biometrischer Daten, die zu den ersten biometrischen Daten passen, und (2) eines zweiten privaten Schlüssels, der zu dem ersten privaten Schlüssel passt, verifiziert wird.

9. Verfahren gemäß Anspruch 8, welches ferner, als Reaktion auf das Empfangen der Anfrage zur Verifizierung der Identität des ersten Individuums, Folgendes umfasst:

Auffordern des ersten Individuums zur Bereitstellung der zweiten biometrischen Daten, die zu den ersten biometrischen Daten passen, und des zweiten privaten Schlüssels, der zu dem ersten privaten Schlüssel passt, wobei die Aufforderung über eine Rechenplattform (104), die mit dem ersten Individuum assoziiert ist, übermittelt wird; oder
Auffordern einer Rechenplattform (104), die mit dem ersten Individuum assoziiert ist, zur automatischen Bereitstellung der zweiten biometrischen Daten, die zu den ersten biometrischen Daten passen, und des zweiten privaten Schlüssels, der zu dem ersten privaten Schlüssel passt.

Revendications

1. Système (100) destiné à réaliser une vérification d'identité personnelle multifactorielle basée sur une chaîne de blocs, le système comprenant :
un ou plusieurs processeurs matériels (126) configurés par des instructions lisibles par machine pour :

établir des adresses de vérification sur une chaîne de blocs par :

l'association d'identificateurs avec des personnes ayant des identités personnelles préalablement vérifiées, un premier identificateur étant associé à une première personne, la première personne ayant une identité personnelle préalablement vérifiée ;
l'affectation d'adresses de vérification sur une chaîne de blocs à des personnes, une adresse de vérification donnée incluant un emplacement spécifique sur la chaîne de blocs où l'information est stockée, dans lequel l'adresse de vérification donnée inclut une clé publique et une clé privée, une première adresse de vérification étant affectée à la première personne, la première adresse de vérification incluant une première clé publique et une première clé privée ; et
l'enregistrement d'identificateurs et de données biométriques associés aux personnes à des adresses de vérification correspondantes, le premier identificateur et les premières données biométriques associés à la première personne étant enregistrés à la première adresse de vérification ; et

la réalisation d'une vérification d'identité personnelle multifactorielle basée sur une chaîne de blocs à l'aide des adresses de vérification par :

la réception d'un ou de plusieurs identificateurs en lien avec une ou plusieurs demandes de vérifier une identité d'une ou de plusieurs personnes, le premier identificateur étant reçu en lien avec une demande de vérifier une identité de la première personne ;
l'extraction des données biométriques associées à la ou aux plusieurs personnes à partir des adresses de vérification correspondantes, les première données biométriques associées à la première personne étant extraites de la première adresse de vérification ; et
la vérification de l'identité de la ou des plusieurs personnes lors de la réception de données biométriques et de clés privées

concordantes, l'identité personnelle de la première personne étant vérifiée lors de la réception (1) de deuxièmes données biométriques concordantes avec les premières données biométriques, et (2) d'une deuxième clé privée concordante avec la première clé privée.

2. Système (100) selon la revendication 1, dans lequel de multiples adresses de vérification sont affectées à des personnes séparées de telle sorte que, en plus de la première adresse de vérification, une deuxième adresse de vérification est affectée à la première personne.

3. Système (100) selon l'une quelconque des revendications précédentes, dans lequel différentes données biométriques sont enregistrées à de multiples adresses de vérification affectées à une personne donnée de telle sorte que, en plus de l'enregistrement du premier identificateur et des premières données biométriques associés à la première personne à la première adresse de vérification, le premier identificateur et des troisièmes données biométriques associés à la première personne sont enregistrés à une troisième adresse de vérification.

4. Système (100) selon la revendication 3, dans lequel l'identité personnelle de la première personne est vérifiée lors de la réception (1) des deuxièmes données biométriques concordantes avec avec les premières données biométriques ou avec les troisièmes données biométriques et (2) de la deuxième clé privée concordante avec la première clé privée.

5. Système (100) selon l'une quelconque des revendications précédentes, dans lequel les données biométriques incluent un ou plusieurs éléments parmi une image, un enregistrement, ou un modèle ; et/ou dans lequel les données biométriques sont en relation avec un ou plusieurs éléments parmi une empreinte digitale, des veines de la paume, la reconnaissance faciale, l'ADN, l'empreinte de la paume, la géométrie de la main, la reconnaissance de l'iris, la rétine, l'odeur ou le parfum, le rythme de frappe, la démarche ou la voix.

6. Système (100) selon l'une quelconque des revendications précédentes, dans lequel le ou plusieurs processeurs matériel (126) sont également configurés par des instructions lisibles par machine pour, en réponse à la réception de la demande de vérifier l'identité de la première personne, inciter la première personne à fournir les deuxièmes données biométriques concordantes avec les premières données biométriques et la deuxième clé privée concordante avec le première clé privée.

7. Système (100) selon l'une quelconque des revendications précédentes, dans lequel au moins un nœud dédié effectue la signature de la vérification de l'identité personnelle de la première personne, dans lequel le nœud dédié inclut un ou plusieurs serveurs (102) du système (100).

8. Procédé destiné à réaliser une vérification d'identité personnelle multifactorielle basée sur une chaîne de blocs à l'aide d'adresses de vérification, le procédé étant effectué par un ou plusieurs processeurs matériels (126) configurés par des instructions lisibles par machine, le procédé comprenant :

la réception d'un ou de plusieurs identificateurs en lien avec une ou plusieurs demandes de vérifier une identité d'une ou de plusieurs personnes, un premier identificateur étant reçu en lien avec une demande de vérifier une identité d'une première personne ;
l'extraction de données biométriques associées à la ou aux plusieurs personnes à partir d'adresses de vérification correspondantes sur une chaîne de blocs, une adresse de vérification donnée incluant un emplacement spécifique sur la chaîne de blocs où l'information est stockée, dans lequel l'adresse de vérification donnée inclut une clé publique et une clé privée, des premières données biométriques associées à la première personne étant extraites à partir d'une première adresse de vérification affectée à la première personne, la première adresse de vérification incluant une première clé publique et une première clé privée ; et
la vérification de l'identité de la ou de plusieurs personnes lors de la réception de données biométriques et de clés privées concordantes, l'identité personnelle de la première personne étant vérifiée lors de la réception (1) de deuxièmes données biométriques concordantes avec les premières données biométriques, et (2) une deuxième clé privée concordante avec la première clé privée.

9. Procédé selon la revendication 8, comprenant également, en réponse à la réception de la demande de vérifier l'identité de la première personne :

l'incitation faite à la première personne de fournir les deuxièmes données biométriques concordantes avec les premières données biométriques et la deuxième clé privée concordante avec la première clé privée, l'incitation étant acheminée via une plateforme informatique (104) associée à la première personne ; ou
l'incitation faite à une plateforme informatique (104) associée à la première personne de fournir automatiquement les deuxièmes données bio-

métriques concordantes avec les première données biométriques et la deuxième clé privée concordante avec la première clé privée.

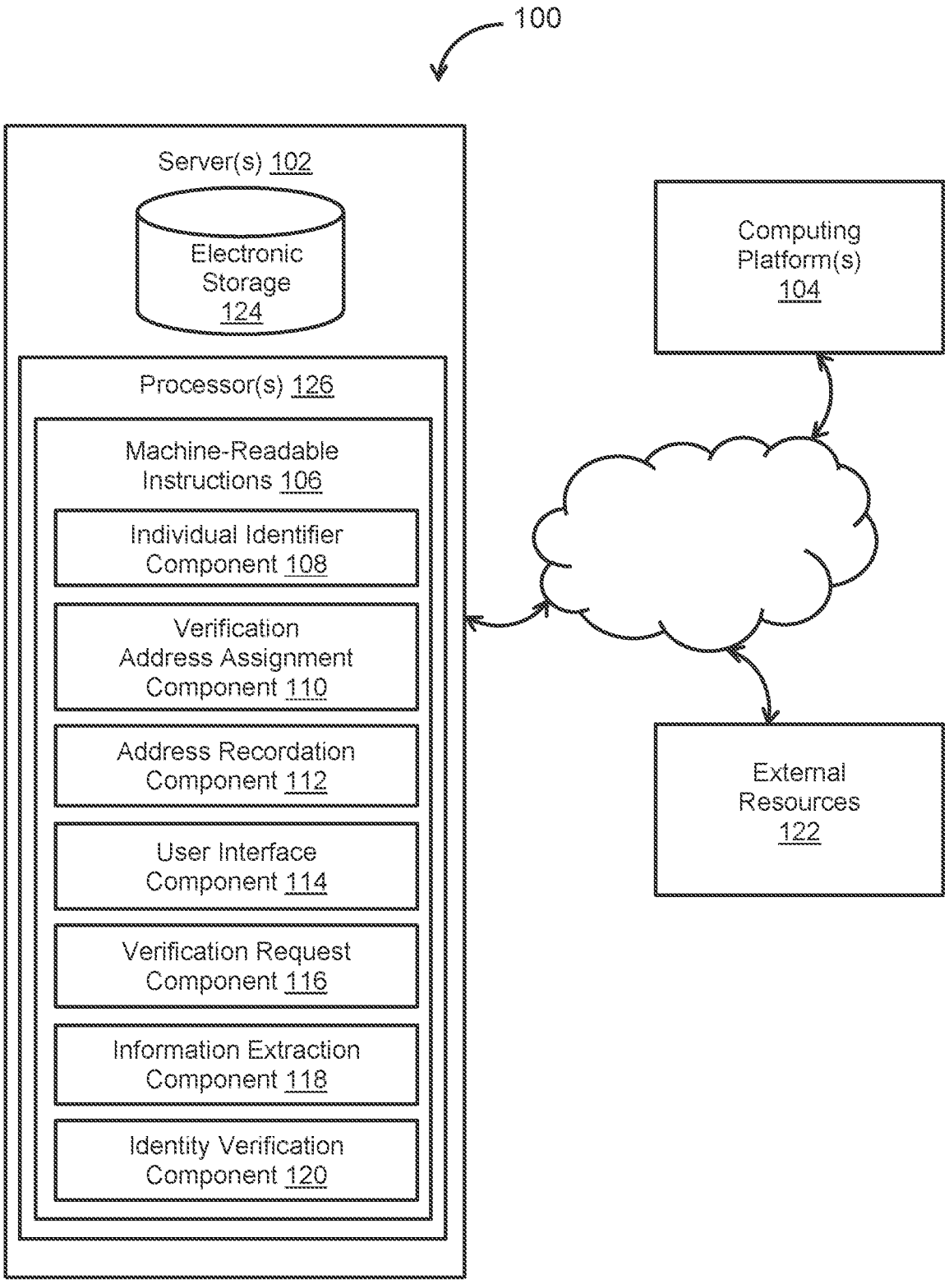
100
Server(s) 102
Electronic Storage 124
Processor(s) 126
Machine-Readable Instructions 106
Individual Identifier Component 108
Verification Address Assignment Component 110
Address Recordation Component 112
User Interface Component 114
Verification Request Component 116
Information Extraction Component 118
Identity Verification Component 120
Computing Platform(s) 104
External Resources 122

FIG. 1

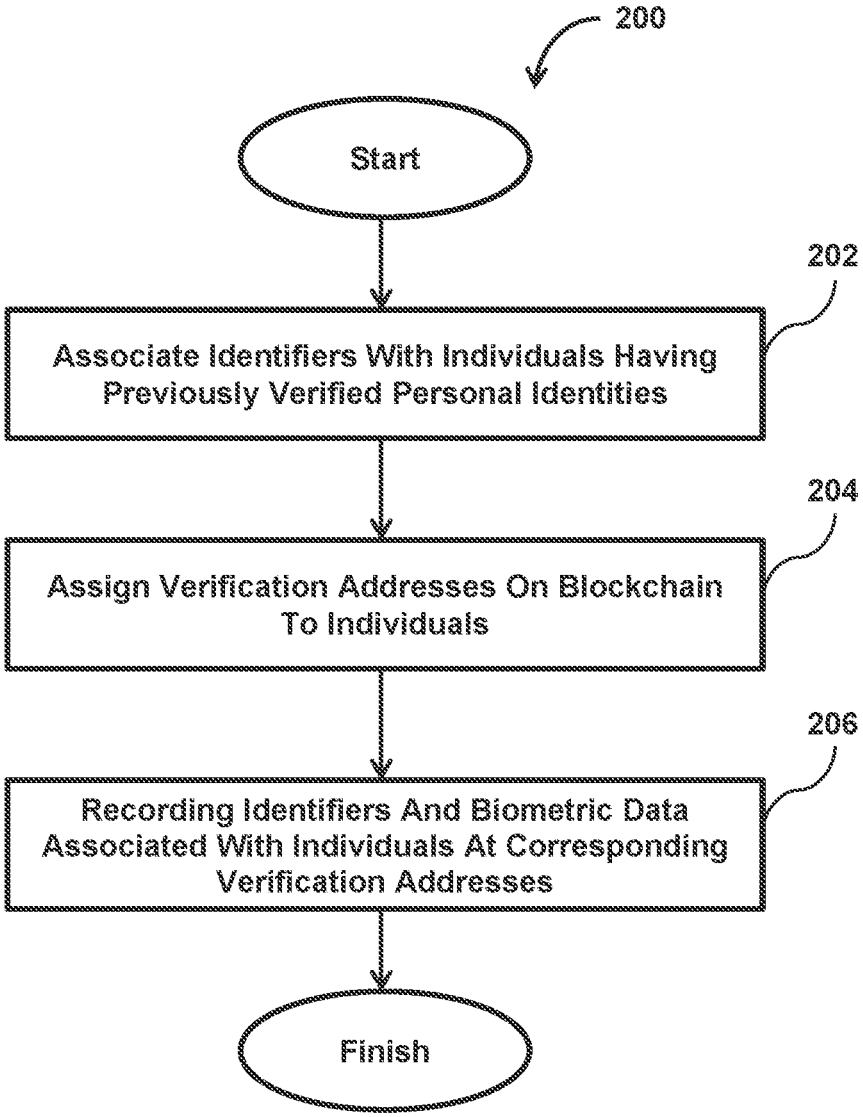
200
Start
202
Associate Identifiers With Individuals Having Previously Verified Personal Identities
204
Assign Verification Addresses On Blockchain To Individuals
206
Recording Identifiers And Biometric Data Associated With Individuals At Corresponding Verification Addresses
Finish

FIG. 2

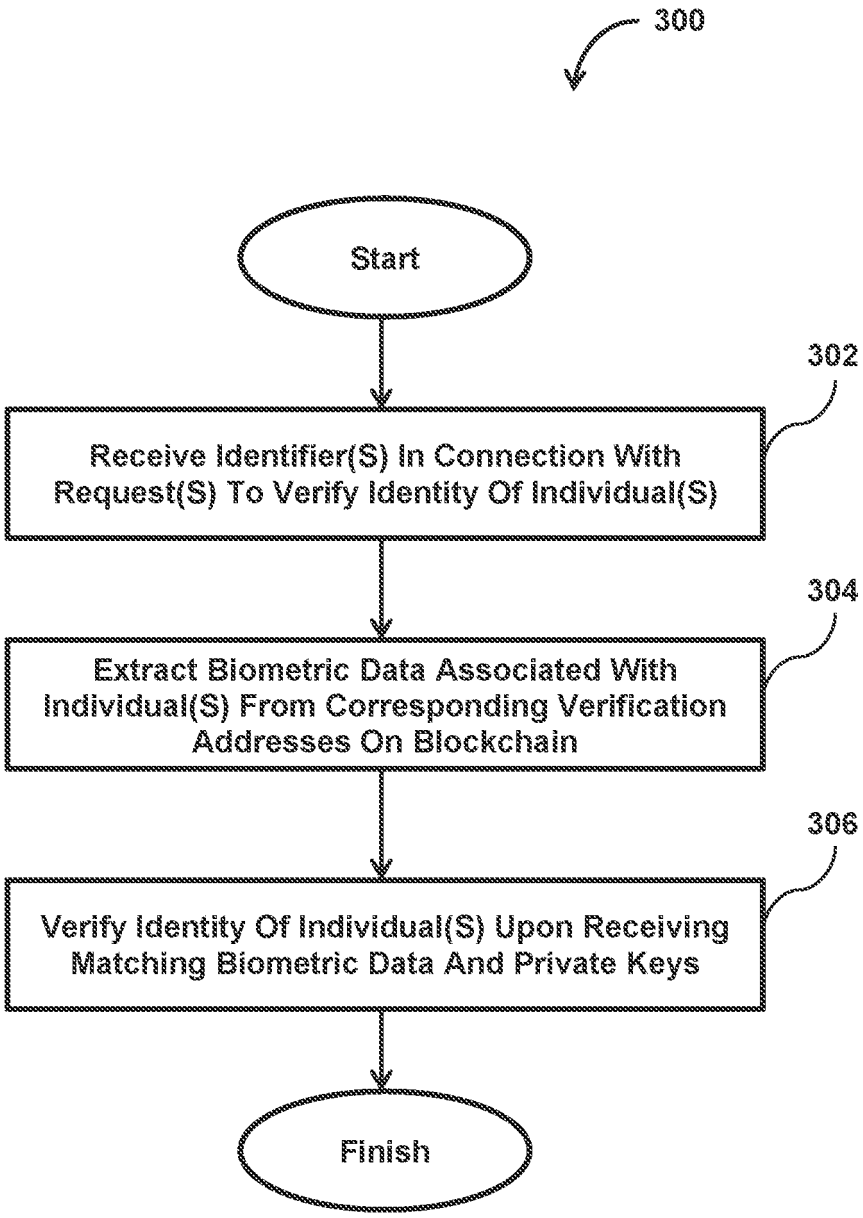
300
Start
302
Receive Identifier(S) In Connection With Request(S) To Verify Identity Of Individual(S)
304
Extract Biometric Data Associated With Individual(S) From Corresponding Verification Addresses On Blockchain
306
Verify Identity Of Individual(S) Upon Receiving Matching Biometric Data And Private Keys
Finish

FIG. 3

REFERENCES CITED IN THE DESCRIPTION

This list of references cited by the applicant is for the reader's convenience only. It does not form part of the European patent document. Even though great care has been taken in compiling the references, errors or omissions cannot be excluded and the EPO disclaims all liability in this regard.

Patent documents cited in the description

- US 20150324789 A1 **[0002]**
- WO 2015183901 A2 **[0003]**